

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

**RECEIVED
FEB - 3 1995**

In the Matter of

Revision of Part 22 of the Commission's
Rules Governing the Public Mobile Services

CC Docket No. 92-115

Amendment of Part 22 of the Commission's
Rules to Delete Section 22.119 and Permit
the Concurrent Use of Transmitters in
Common Carrier and Non-common Carrier
Service

CC Docket No. 94-46
RM 8367

Amendment of Part 22 of the Commission's
Rules Pertaining to Power Limits for Paging
Stations Operating in the 931 MHz Band in
the Public Land Mobile Service

CC Docket No. 93-116

TO: THE COMMISSION

JOINT REPLY AND COMMENT

**THE CELLULAR COMMUNICATIONS
INDUSTRY ASSOCIATION**

**THE MOBILE AND PERSONAL
COMMUNICATIONS DIVISION
OF THE TELECOMMUNICATIONS
INDUSTRY ASSOCIATION**

on

**Michael F. Altschul
Randall S. Coleman
Andrea D. Williams
1250 Connecticut Ave., N.W.
Suite 200
Washington, D.C. 20036**

**Grier C. Raclin, Esq.
Anne M. Stamper, Esq.
Gardner, Carton & Douglas
1301 K Street, N.W.
Suite 900, East Tower
Washington, D.C. 20005**

**Eric J. Schimmel; Vice President
Jesse Russell; Chairman, Mobile and
Personal Communications
Division
Telecommunications Industry
Association
2500 Wilson Blvd.
Suite 300
Arlington, Virginia 22201**

Dated: February 2, 1995

RECEIVED

FEB - 3 1995

FEDERAL COMMUNICATIONS COMMISSION

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of)	
)	
Revision of Part 22 of the Commission's)	CC Docket No. 92-115
Rules Governing the Public Mobile Services)	
)	
Amendment of Part 22 of the Commission's)	CC Docket No. 94-46
Rules to Delete Section 22.119 and Permit)	RM 8367
the Concurrent Use of Transmitters in)	
Common Carrier and Non-common Carrier)	
Service)	
)	
Amendment of Part 22 of the Commission's)	CC Docket No. 93-116
Rules Pertaining to Power Limits for Paging))	
Stations Operating in the 931 MHz Band in)	
the Public Land Mobile Service)	

JOINT REPLY AND COMMENT

The Mobile and Personal Communications Division of the Telecommunications Industry Association ("TIA"), and the Cellular Telecommunications Industry Association ("CTIA") (hereinafter jointly called the "Parties"), by their counsel and pursuant to Section 1.429(g) of the Commission's Rules, 47 C.F.R. § 1.429(g) (1994), hereby jointly provide this Reply and Comment in the above-referenced proceeding. In support hereof, the Parties state as follows:

I. BACKGROUND

1. On August 2, 1994, the Commission adopted a *Report and Order* in this proceeding, implementing new Section 22.919 of the Commission's Rules to address the problem of cellular fraud.^{1/} New Section 22.919 of the Rules establishes cellular equipment design specifications which require, among other things, that cellular equipment's Electronic Serial Numbers ("ESNs") must be set at the equipment's manufacturing site, and must not be alterable, transferable, removable or otherwise able to be manipulated by any party "in the field."^{2/} The Commission declined to make an exception to Rule 22.919 requested by some TIA members, which would have allowed manufacturers' authorized agents to transfer ESNs in normal repair activities,^{3/} and also declined to require that new mobile cellular equipment comply with industry authentication standards.^{4/}

2. On December 19, 1994, TIA petitioned the Commission to reconsider its decision insofar as it prohibited manufacturers' authorized service centers or representatives from transferring ESNs in connection with the normal repair and upgrade of cellular mobile equipment.^{5/} In addition, TIA requested the Commission to require cellular mobile equipment receiving type-acceptance approval after September, 1995 to conform with industry authentication standards.^{6/} TIA's Petition was supported by

^{1/} *In the Matter of Revision of Part 22 of the Commission's Rules Governing the Public Mobile Services, Report and Order*, CC Docket No. 92-115, 9 FCC Rcd. 6513 (1994) (the "*Report and Order*").

^{2/} *Report and Order*, 9 FCC Rcd at 6525, ¶¶54-63.

^{3/} *Id.* at ¶ 61.

^{4/} *Id.* at ¶ 59.

^{5/} TIA's Petition did not oppose the prohibition of ESN alteration by persons other than manufacturer's authorized agents.

Matsushita Communications Industrial Corporation on January 20, 1995, and a Petition making some of the same comments was filed on December 19, 1994 by the Ericsson Corporation.

3. On January 20, 1995, CTIA filed an Opposition to TIA's request to allow repair centers to undertake ESN transfers, but supported industry efforts to require that next generation cellular telephones include authentication features.^{2/} Indeed, to the Parties' knowledge, no party opposed TIA's request that future cellular equipment be required to incorporate authentication features conforming to TIA's standards.

II. SUMMARY OF JOINT REQUEST

4. After the filing of the above-referenced pleadings, representatives of the Parties, including GTE Laboratories (CTIA's engineering consultant on anti-fraud matters), met numerous times in person and/or over the telephone in an attempt to resolve the differences that appeared to exist in their respective filings. The Parties agreed during these meetings that cellular fraud should be fought by every reasonable means, and it appears from these meetings that the only significant issue between the Parties related to a manufacturer's ability to upgrade and otherwise manipulate a mobile unit's operating software without compromising the industry's efforts to combat cellular fraud. As TIA previously has explained, the ESN-based solution adopted in Section 22.919 could adversely affect certain repair activities undertaken by manufacturers. Further discussion between the Parties revealed that these concerns apparently could be addressed, without undermining the Parties' or the Commission's ability to

^{b/} TIA also requested the Commission to clarify that manufacturers' authorized agents may transfer ESNs in connection with the repair and upgrade of equipment for which initial type-acceptance was sought before January 1, 1995. *TIA Petition* at ¶ 9. CTIA did not address this request in its Opposition.

^{2/} *CTIA Opposition/Comments* at 4 and 7.

fight cellular fraud, through the adoption of minor changes to Rule Section 22.919. The Parties jointly offer this Reply and Comment to set forth and describe the minor changes they have agreed to in order to address these concerns.^{8/}

5. TIA and CTIA herein request the Commission to modify Rule 22.919 in accordance with the draft Rule Section 22.919 set forth as Attachment A hereto. Specifically, the Parties request the Commission to (a) require that cellular mobile equipment receiving Type Acceptance approval after July 1, 1995 comply with industry authentication standards, and (b) allow manufacturers^{9/} to transfer ESNs in connection with normal repair and service upgrade activities *provided that* (i) the unit's original factory-set ESN is utilized at all times to uniquely identify the unit, and (ii) if the unit has been activated for service on a carrier's system, any transfer of an ESN assigned to that unit must take place at a location owned and operated by the unit's manufacturer. The proposed Rule also clarifies some confusion surrounding the Commission's original section 22.919 by making it clear that a unit's manufacturer may program a new factory-set ESN into a unit that is returned to the manufacturer for repair or "remanufacturing."

III. MANDATORY AUTHENTICATION

6. As set forth in TIA's Petition, and supported by CTIA and others, authentication offers an effective means of protecting against cellular fraud. As described in TIA's Petition, non-authenticating cellular phones transmit their unencoded ESNs over the air during call set-up procedures. These ESNs are subject to interception by unauthorized users, who may pirate and insert the ESNs into units that

^{8/} Concurrently herewith, TIA is filing a *Motion for Extension of Time* to allow TIA and CTIA further time to discuss and propose to the Commission additional changes to its Rules to better protect against cellular fraud.

^{9/} The scope of the term manufacturer includes manufacturers' commonly owned and controlled affiliates.

effectively become “clones” of the authorized phones, thus allowing the fraudulent misdirection of call billing information. Authentication addresses this problem by not transmitting the data needed for billing verification over-the-air in a fashion subject to interception and misuse.

7. Authentication was introduced by TIA in 1989 as an effective way to attack cellular access fraud. The authentication procedures incorporated into TIA’s standards^{10/} were based upon well-established authentication methodologies previously adopted for use in the European Global System for Communications (GSM) networks, and which have been universally applauded for their effective security against access fraud. Additionally, the authentication standards adopted by TIA may be applied to all established air-interfaces of cellular access technologies, including analog, TDMA, and CDMA.

8. The authentication procedure called for in TIA’s specifications provides for an exchange of information -- a simple challenge-response scheme -- between an “Authentication Center” (“AC”) associated with the relevant carrier network, and cellular telephones seeking to use that carrier’s system. The TIA authentication protocol occurs during telephone registration, at call origination, at call termination (incoming), and at other times as specified by the carrier. Pursuant to this protocol, a legitimate cellular telephone and the AC share a common cryptographic algorithm and secret cryptographic “key” that allow them to compute the same result from a given random number challenge. The challenge-response technique in its most general form, provides for the cellular system to generate a non-predictable (random) number “challenge” that is sent to both the AC and, via an ‘clear’ (not encoded) over-the-air interface, to the relevant cellular telephone. The cellular telephone then computes an authentication response using the authentication algorithm and a secret cryptographic key; and

^{10/} See TIA IS-41 (inter-system signaling-1992); IS-54B (TDMA Dual Mode phones - 1992); IS-95 (CDMA Dual Mode phones - 1993); IS-91 (AMPS and NAMPS analog phones - 1994); and IS-136 (TDMA Single Mode Telephones - adoption pending).

transmits that response through the cellular network to the AC, where the AC tests the validity of the subscriber by comparing the received response with one it computes. If the response proves valid, the cellular system will allow cellular system access and can be confident that the subscriber is legitimate. If the response is invalid, the system may deny access with equal confidence. If a unit's A-key consists of 64 bits, it would take a potential fraudulent actor, using a computer incorporating a "486" processor, nearly *3 million years* to decode the A-key. Even given this high level of security, the security protocols also provide a mechanism to update certain cryptographic keys used in the system.

9. Contrary to the Commission's expressed fears,^{11/} the adoption of authentication methodologies outlined in TIA's standards will not undercut the ability of carriers to implement switch-based cellular extension telephone service. Cellular extension service generally consists of two or more cellular phone units functioning with the either same MIN and unique ESNs; or different MINs and unique ESNs, all of which are associated with a single billing party. In either case, the introduction of authentication would require only the addition of a unique authentication key for each cellular phone unit. Moreover, the industry through TIA has approved standards for the latter type of cellular extension service that incorporates the use of "cellular hunt groups." This process allows the system to prioritize the calling order of associated MINs or to page multiple associated MINs simultaneously. Given the various methods of offering switch-based cellular extension service consistent with the use of authentication techniques, and the industry's overall support of the adoption of authentication methodologies to aid in the prevention of cellular fraud, there simply is no reason for the Commission to

^{11/} *Report and Order* at ¶ 59

reject the proposed authentication mandate on the basis of the unfounded concern that switch-based cellular extension services would be undermined

10. Commission endorsement of mandatory authentication standards will substantially facilitate the implementation of authentication as a cellular fraud fighting tool.^{12/} Accordingly, the failure to standardize and implement authentication as described in TIA standards will potentially eliminate and, at least, greatly delay the implementation of a proven method of successfully attacking cellular fraud.

IV. RULE CHANGES REQUIRED TO ALLOW CERTAIN REPAIR AND UPGRADE ACTIVITIES

11. In addition to the adoption of mandatory authentication requirements outlined above, the Parties also request the Commission to adopt certain minor changes to Rule Section 22.919 that are required to allow manufacturers to undertake certain unit repair and upgrade activities without compromising the effectiveness of the FCC's anti-fraud rules.

12. The ESN information of many cellular telephones used today is not isolated from, but is integrated with, the units' other operating software as anticipated by Section 22.919 of the Rules.^{13/} In the repair and upgrade of these telephones, the telephones' operating software -- which may include the ESN -- is removed from the unit, and new corrected or upgraded software along with the original ESN is

^{12/} Antitrust restrictions can sometimes work to prohibit competitors from agreeing upon standards to govern their products, but these concerns are eliminated to the extent the standards are reviewed, approved and actually implemented by governmental agencies, such as the FCC. See *California Motor Transport v. Trucking Unlimited*, 404 U.S. 508 (1972); *United Mine Workers v. Pennington*, 381 U.S. 657 (1965), cert. denied, 393 U.S. 983 (1968); *Eastern R.R. Presidents Conference v. Noerr Motor Freight Inc.*; 365 U.S. 127 (1960) (the "Norrr-Pennington doctrine").

^{13/} Section 22.919 provides that "[i]f the ESN host component contains other information, the ESN must be encoded using one more of the following techniques " 47 C.F.R. § 22.919(b)(1995).

then inserted into the telephone. Because the ESN is an integral part of the units operating software, the ESNs in these units must be removed temporarily during repair and upgrade procedures to allow the repair or upgrade to occur. Section 22.919 of the Rules, as presently written to prohibit any ESN transfer or manipulation, would appear to prohibit these repair and upgrade activities in the field and board replacement activities suggested by CTIA in its *Opposition*

13. The proposed revised rule, Attachment A, attempts to address this problem by allowing the *manufacturer* (but not independent agents or other parties) to *transfer* (not change, alter or modify) ESNs in connection with these repair and upgrade activities. Moreover, the Rule protects the ESN-transferring software from misuse by requiring that ESN transfers occur only *at locations owned and operated by the unit's manufacturer*, if repair and upgrade activities are required in connection with telephones that have already been activated by a carrier.^{14/} In addition, the revised Rule makes explicit what was previously stated only in paragraph 62 of the *Report and Order* adopting 22.919: that the operation of a cellular mobile telephone incorporating an ESN other than that set by the manufacturer in compliance with the Rule is prohibited.^{15/}

14. After exhaustive discussion and negotiation, the Parties believe, and respectfully suggest to the Commission, that the suggested revisions to Rule 22.919 strike the proper balance between the desire to take all reasonable steps to fight cellular fraud, and the industry's need to be able to undertake

^{14/} The revised Rule allows ESN transfers by manufacturers other than at manufacturers' locations because some repairs or upgrades involve *many thousands* of units and it is infeasible to require that such volumes of units be returned to the unit's manufacturer for repair and upgrade activities.

^{15/} To allow the exchange of ESNs from defective units, the revised Rules provides a single exception to this provision, allowing manufacturers to insert new ESNs into units that have been returned to the manufacturer for repair and are subsequently remanufactured.

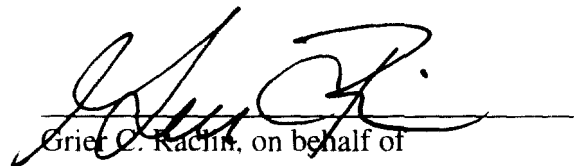
reasonable repair activities in circumstances that will protect ESN-transferring software from misuse.

The revised Rule would allow ESN transfers *only* by manufacturers, and *only* at protected locations if the units have been activated, and makes explicit that the operation of units incorporating ESNs that are transferred in noncompliance with this Rule is prohibited.

IV. CONCLUSION

15. For the foregoing reasons, therefore, the Mobile and Personal Communications Division of the Telecommunications Industry Association, and The Cellular Communications Industry Association, respectfully request the Commission to revise 22.919 of the Commission Rules in accordance with Attachment A hereto.

Respectfully submitted,



Grier C. Raclin, on behalf of

THE CELLULAR COMMUNICATIONS INDUSTRY ASSOCIATION

**Michael F. Altschul
Randall S. Coleman
Andrea D. Williams**

**1250 Connecticut Ave., N.W.
Suite 200
Washington, D.C. 20036**

Its Attorneys

THE MOBILE AND PERSONAL COMMUNICATIONS DIVISION OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

**Grier C. Raclin, Esq.
Anne M. Stamper, Esq.**

**Gardner, Carton & Douglas
1301 K Street., N.W.
Suite 900, East Tower
Washington, D.C. 20005**

Its Attorneys

**Eric J. Schimmel; Vice President
Jesse Russell; Chairman, Mobile and
Personal Communications
Division
Telecommunications Industry
Association
2500 Wilson Blvd.
Suite 300
Arlington, Virginia 22201**

Dated: February 2, 1995

ATTACHMENT A

PROPOSED RULE SECTION 22.919

The Electronic Serial Number (ESN) is a 32 bit binary number that uniquely identifies a cellular mobile transmitter to any cellular system.

- (a) Each mobile transmitter in service must have a unique ESN.
- (b) The ESN host component must be permanently attached to a main circuit board of the mobile transmitter and the integrity of the unit's operating software must not be alterable except by the mobile unit's manufacturer, or its commonly owned and controlled affiliate, in conformance with subsection (c) of this Rule. The ESN must be isolated from fraudulent contact and tampering. If the ESN host component does not contain other information, that component must not be removable, and its electrical connections must not be readily accessible except by the unit's manufacture, or its commonly owned and controlled affiliate, in compliance with this Rule section. If the ESN host component contains other information, the ESN must be encoded using one or more of the following techniques:
 - (1) Multiplication or division by a polynomial;
 - (2) Cyclic coding;
 - (3) The spreading of ESN bits over various non-sequential memory locations.
- (c) The ESN must be factory-set and must not be alterable, transferable, removable or otherwise able to be manipulated except that the manufacturer of the mobile transmitter, or its commonly owned and controlled affiliate, may manipulate the operating software of the transmitter, which may include the ESN, provided that the unit's original factory-set ESN is utilized at all times to uniquely identify the transmitter to any cellular system. Manipulation of the operating software by the manufacture, or its commonly owned and controlled affiliate, shall only occur: (i) at a facility owned and operated by the manufacturer or its commonly owned and controlled affiliate; or (ii) with respect to mobile transmitters that have never been activated for use on a cellular system, by an employee of the manufacturer or its commonly owned and controlled affiliate. Nothing in this section shall prohibit the original manufacturer or its commonly owned and controlled affiliate from programming a new factory-set ESN into a remanufactured unit, provided that the new ESN uniquely identifies the transmitter to any cellular system. Cellular mobile equipment must be designed such that any attempt to remove, tamper with, or change the ESN chip, its logic system, or firmware originally programmed by the manufacturer, other than in compliance with this Rule section, will render the mobile transmitter inoperative
- (d) Cellular mobile transmitters receiving Type Acceptance approval after July 1, 1995 must comply with industry standards for authentication key and signature calculation procedures and error interface capability specifications established by the Telecommunications Industry Association (TIA).
- (e) No mobile transmitter may be operated utilizing an ESN other than that programmed into the unit by its manufacturer.

CERTIFICATE OF SERVICE

I, Christine Peyton, a secretary in the law firm of Gardner, Carton & Douglas, certify that I have this 3rd day of February, 1995, caused to be sent by first-class, U.S. mail, postage prepaid, a replacement copy of the foregoing **MOTION FOR EXTENSION OF TIME** to the following:

Michael F. Altschul
Vice President, General Counsel
Cellular Telecommunications Industry Association
1250 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20036

Randall S. Coleman
Vice President, Regulatory Policy and Law
Cellular Telecommunications Industry Association
1250 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20036

Andrea D. Williams
Staff Counsel
Cellular Telecommunications Industry Association
1250 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20036

Timothy J. Fitzgibbon
Thomas F. Bardo
Carter, Ledyard & Milburn
1350 I Street, N.W., Suite 870
Washington, D.C. 20005

MTC Communications
Box 2171
Gaithersburg, MD 20886
Attn: M.G. Heavener, President

Christine Peyton
Christine Peyton